LDRD Project Description and Rationale for Approach

Current Implementation & Savings:

Estimated Savings: The INEEL has implemented a form of database electronic signatures in the Transuranic Reporting and Inventory Processing System (TRIPS) database. This system is highly data intensive. The system, when implemented, will contain information on up to 140,000 waste containers. There is a large amount of output from instruments, creating about 1,000 pages of typed and hand written documents per waste container. At least six levels of data reviews and approvals occur, with different personnel involved at each level. As many as 40,000 signatures per year may be generated. In the past, this data was gathered using paper based forms and with written comments and signatures on each form. The TRIPS system as a whole will virtually eliminate the need for storing and tracking 900,000 paper copies of signed reports per year. The INEEL Site Program Office (SPO) estimates a paper based record system will cost $9M through the year 2002. Although, the costs comparing a TRIPS paper-based record system to the TRIPS digital signature system has not been studied, other similar studies have been completed. One such study published by President Clinton's Management Council and its Electronic Processing Initiatives Committee (EPIC) compared a paper-based transaction model with the smart card based digital signature transaction model. This study, as described in the Federal Smart Card Implementation Plan, noted that the processing costs of the paper-based model were $120/transaction. The processing costs of the smart card based digital signature model were $18/transaction, savings of 85% over the paper-based model.

Current Implementation: This system is very tightly coupled to the TRIPS database application and provides the capability of producing, verifying, and tracking digital signatures. Inherent within each signature is the ability to determine who created the signature as well as validate the data currently stored within the database against the data recorded at signing. The module utilizes industry standard public key cryptographic algorithms and infrastructure to provide the digital signature functions. As part of the public key infrastructure, a Certificate Authority (CA) is used to create and distribute a user's public key certificate, and a smart card is used to store the corresponding private key. In PKCS, the public and private keys are algorithmically related. To control the ability to sign, a Certificate Revocation List (CRL) is used to track expired or revoked user certificates. If a user's certificate is contained in the CRL, they are not allowed to sign new data. Historical signatures can always be validated, even those in the CRL.

To create a digital signature, the system uses the signer's private key and a snapshot of data extracted from the database. The snapshot is analogous to a paper report in a paper-based system. To verify a signature against the current data in the database, the system uses the public key obtained from the signer's certificate, the digital signature stored within the database (using PKCS#1 standard signatures), and a new snapshot created from an identical data extraction process. The system stores the original snapshots in specially-designed the Lightweight Directory Access Protocol (LDAP) database for scalability, portability, and efficiency. This provides a historical signature trail and provides a signature verification mechanism independent of database data changes. Since LDAP is an Internet standard, it is also well suited to support distributed work forces that require signature and data authentication independent of access to the original database used to store the data.

To manage the keys and guarantee user authenticity, a certificate database and a smart card is required. The certificate database is the main repository of the public keys and is implemented in a standard, network X.500 database accessed via LDAP. The certificate database stores a history of all certificates issued so **signatures can be verified even after the certificate is "revoked" and the user is no longer permitted to sign new data**. The smart card stores both the private key and certificate of an individual using Public Key Cryptography Standard#11 (PKCS#11) functions. Each person needing the ability to sign is required to have a smart card. No special hardware is required for verifying. From a user's perspective, the only interaction required to sign is to enter their unique user PIN to access their smart card (i.e., User PIN + User Smart Card + Internal Application of Signature Algorithm -*replaces*- Writing an Ink Signature on Paper).

To verify, a user would only be required to initiate the verification mechanism, i.e., push the verification button, and is not required to have a smart card or a certificate / private key.

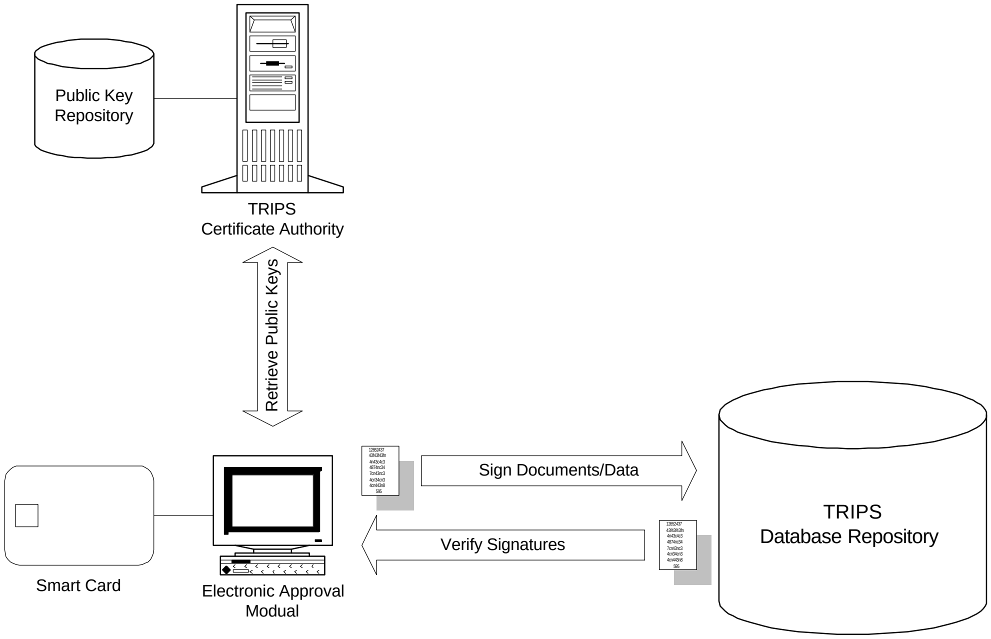

Figure 1. Overview of creating / verifying a digital signature.